



**Homeland
Security**

Daily Open Source Infrastructure Report

30 July 2015

Top Stories

- About 15 million gallons of water spilled out after a 54-inch pipe broke at the Crystal Springs reservoir July 27 in San Bruno that went unfixed for over 13 hours. – *KRON 4 San Francisco* (See item [18](#))
- The governor of Oregon ordered State agencies July 28 to reduce water consumption by at least 15 percent or more on average across all State-owned. – *Reuters* (See item [20](#))
- An alleged self-professed Islamic State adherent was charged with attempting to use a weapon of mass destruction against a person or property within the U.S. July 28 after planning to remotely detonate a timer bomb on a public beach in Key West. – *U.S. Department of Justice* (See item [25](#))
- Investigators involved in a previously unreported May or June breach of United Airlines' computer systems reported links between the hackers and the Chinese threat group that breached the records from the U.S. Office of Personnel Management, Anthem Inc., among other organizations. – *Bloomberg* (See item [35](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. ***July 29, Forum News Service*** – (North Dakota; Idaho) **\$900,000 fine for violating oil field regulations.** The North Dakota Industrial Commission fined Idaho-based Alturas Energy LLC \$900,000 July 28 in response to 12 alleged oil regulation violations, including 2 unresolved saltwater spills.
Source: <http://www.jamestownsun.com/news/state/3806757-900000-fine-violating-oil-field-regulations>
2. ***July 29, KETV 7 Omaha*** – (Nebraska) **Emergency crews respond to fuel leak in Bennington.** Hazmat crews responded to a fuel spill at a gas station in Bennington, Nebraska July 29 after safety measures failed to prevent the overfill of a 5,000 gallon tanker truck. At least 1,000 gallons of fuel were leaked and may have entered a nearby storm system, forcing crews to block portions of Highway 36 for nearly 5 hours.
Source: <http://www.jamestownsun.com/news/state/3806757-900000-fine-violating-oil-field-regulations>
3. ***July 28, KWCH 12 Hutchinson*** – (Oklahoma) **Oil wells shut down near Crescent, Okla. following multiple earthquakes Monday.** The Oklahoma Corporation Commission announced July 28 the shutdown of two wells and reduced injection at a third well near Crescent, Oklahoma after five earthquakes hit the area July 27.
Source: <http://www.kwch.com/news/local-news/oil-wells-shutdown-near-crescent-okla-following-multiple-earthquakes-monday/34380634>
4. ***July 28, Nashville Tennessean*** – (Tennessee) **Storm leaves 30,000 without power, planes stuck at Nashville airport.** Approximately 30,000 Nashville Electric Service customers lost power July 28, including parts of Nashville International Airport where workers believe a lightning strike affected jet bridges attached to departing planes, leaving them nonoperational.
Source: <http://www.tennessean.com/story/weather/2015/07/28/severe-t-storm-warning-heat-advisory-parts-midstate/30798163/>
5. ***July 28, Arizona Daily Star*** – (Arizona) **Storms flood washes, cause scattered power outages.** Tucson Electric Power crews were working to restore power July 28 to 20,000 customers after severe storms downed power lines, flooded streets, and delayed several flights at Tucson International Airport.
Source: http://tucson.com/news/local/storms-flood-washes-cause-scattered-power-outages/article_a4788d42-3583-11e5-a0ab-77716f614cf9.html
6. ***July 27, WNEP 16 Scranton*** – (Pennsylvania) **Oil spill cleanup at school.** The U.S. Department of Environmental Protection (DEP) is monitoring Panther Valley High School for odors or Volatile Organic Compounds after approximately 5,000 gallons of heating oil were spilled from an underground storage tank at nearby Panther Valley Middle School in Carbon County, Pennsylvania July 27. The cause of the leak is being investigated and school officials are cooperating with the DEP to prevent the oil from reaching nearby wetlands.
Source: <http://wneplive.com/2015/07/27/oil-spill-cleanup-at-school/>

For another story, see item [32](#)

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

7. *July 28, U.S. Department of Labor* – (Georgia) **Georgia metal fabrication installer fails to protect workers from dangerous falls.** The Occupational Safety and Health Administration cited Cairo-based Ansley Metal Fabrication and Repair July 28 with 1 willful and serious safety violation for exposing workers to fall hazards of up to 30 feet by not ensuring employees were properly using fall protection equipment. Proposed penalties total \$53,900.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28347

8. *July 28, WTAE 4 Pittsburgh* – (Pennsylvania) **Chemical spill results in 17 plant workers going through decontamination process.** Seventeen workers at Prime Metals & Alloys in Homer City were treated, and one was hospitalized following a chemical spill at the facility.

Source: <http://www.wtae.com/news/chemical-spill-results-in-plant-workers-going-through-decontamination-process-in-homer-city/34401766>

For another story, see item [32](#)

Defense Industrial Base Sector

For additional stories, seem items [23](#) and [32](#)

Financial Services Sector

9. *July 29, Associated Press* – (International) **Floridian last of 12 convicted in Texas for timeshare fraud.** A Florida man was convicted July 28 for leading a \$10 million timeshare scam in the U.S. and Canada in which he scammed over 5,000 timeshare owners by hiring telemarketers to solicit fees in false buying promises. Eleven other suspects have pleaded guilty in connection to the scheme.
- Source: <http://www.thenewstribune.com/news/business/article29271061.html>
10. *July 28, Montgomery News* – (Pennsylvania) **Two sought for allegedly stealing more than \$100K through fraudulent credit card accounts.** Authorities reported July 28

that they are seeking the owners of the Fort Washington-based Centra-Spike heating, ventilation, and air conditioning company on charges that the pair allegedly stole \$124,981 by using stolen identities of at least 8 victims to obtain fraudulent loans.

Source:

http://www.montgomerynews.com/articles/2015/07/28/ambler_gazette/news/doc55b7b4e598593326989643.txt

11. ***July 28, Reuters* – (National) Western Union's Paymap to pay \$38.4 mln over mortgage ads.** The U.S. Consumer Financial Protection Bureau reported July 28 that Paymap Inc., a unit of Western Union Co., agreed to pay \$38.4 to resolve U.S. regulatory allegations that the company deceived consumers into signing up for a LoanCare LLC program that promised false savings. LoanCare LLC will pay a \$100,000 civil fine, and both companies agreed not to advertise the mortgage program's benefits without providing supporting evidence.
Source: <http://www.reuters.com/article/2015/07/28/sec-paymap-settlement-idUSL1N10827Q20150728>

For additional stories, see items [21](#) and [32](#)

Transportation Systems Sector

12. ***July 29, Associated Press* – (Ohio) I dead, 10 injured as church van crashes into train in Ohio.** A van carrying vacation Bible school students crashed through a crossing gate into the side of a freight train at a rail crossing in Middletown, Ohio, killing an adult passenger and injuring 9 children and the driver July 29. The Ohio State Highway Patrol reported that gates were down and warning lights were activated at the crossing during the time of the accident.
Source: <http://abcnews.go.com/US/wireStory/woman-dies-kids-injured-van-crashes-train-ohio-32754519>
13. ***July 29, WCNC 36 Charlotte* – (Indiana; North Carolina) Plane with Carolina Panther on board makes emergency landing.** An American Airlines plane headed to Charlotte from Chicago made an emergency landing July 28 to Indianapolis after the plane showed indication of a mechanical issue. The plane landed safely and was cleared to fly after being checked by an Indiana Mechanical Team.
Source: <http://www.wcnc.com/story/news/2015/07/29/plane-with-carolina-panther-on-board-makes-emergency-landing/30819511/>
14. ***July 28, West Volusia Beacon* – (Florida) Truck driver killed after semi strikes I-4 guardrail, overturns, FHP says.** Interstate 4 between Daytona Beach and State Road 44 was shut down for approximately 2 hours July 27 after a semi-truck crashed into a guardrail and overturned, killing the driver.
Source: <http://beacononlinenews.com/news/daily/7311>

For additional stories, see items [2,4,5](#), and [35](#)

Food and Agriculture Sector

15. *July 29, Associated Press* – (California) **California fines 6 companies selling tainted produce.** California State officials reported July 28 that six companies based in Los Angeles and San Mateo counties imported produce contaminated with illegal pesticide residues from Thailand, Taiwan, China, and Mexico to State residents after ignoring warnings and repeatedly selling the tainted products. Each company paid fines up to \$20,000.
Source: <http://www.washingtontimes.com/news/2015/jul/29/california-fines-6-companies-selling-tainted-produ/>
16. *July 27, U.S. Food and Drug Administration* – (National) **KellBran Candies issues allergy alert on undeclared milk in Caramel Popcorn.** KellBran Candies, an Akron, Ohio establishment, is recalling KellBran Caramel Popcorn due to an undeclared milk allergen July 27. The product was distributed to various retail specialty grocery stores nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm456160.htm>
17. *July 25, U.S. Food and Drug Administration* – (National) **Kroger recalls four seasonings due to possible health risk.** Kroger Co. of Cincinnati, Ohio is recalling Kroger Ground Cinnamon, Kroger Garlic Powder, Kroger Coarse Ground Black Pepper, and Kroger Bac'n Buds due to possible Salmonella contamination July 25. The products were sold to retail stores nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm456182.htm>

For another story, see item [32](#)

Water and Wastewater Systems Sector

18. *July 28, KRON 4 San Francisco* – (California) **15 million gallons of water wasted.** About 15 million gallons of water spilled out after a 54-inch pipe broke at the Crystal Springs reservoir July 27 in San Bruno. Officials reported that the water leak went unfixed for over 13 hours in order to ensure that water pressure in surrounding neighborhoods would not be affected.
Source: <http://kron4.com/2015/07/28/15-million-gallons-of-water-wasted-in-san-bruno-water-main-break/>
19. *July 28, HawaiiNewsNow* – (Hawaii) **5,000 gallons of wastewater overflows in Lahaina.** Roughly 5,000 gallons of wastewater overflowed July 28 in Lahaina, Maui, due to a wire failure at a pump station. The area has been cleaned and disinfected, and warning signs were posted.
Source: <http://www.hawaiinewsnnow.com/story/29653378/5000-gallons-of-wastewater-overflows-in-lahaina>
20. *July 28, Reuters* – (Oregon) **Oregon Governor orders State agencies to reduce water consumption.** The governor of Oregon ordered State agencies to reduce water consumption by at least 15 percent or more on average July 28 across all State-owned

facilities on or before December 31, 2020. The executive order comes as the governor has declared drought emergencies for 23 of the State's 36 counties.

Source: <http://www.reuters.com/article/2015/07/28/usa-oregon-drought-idUSL1N10835R20150728>

Healthcare and Public Health Sector

21. ***July 28, U.S. Securities and Exchange Commission – (International) SEC charges Mead Johnson Nutrition with FCPA violations.*** The U.S. Securities and Exchange Commission announced July 28 a \$12 million settlement with Mead Johnson Nutrition Company over allegations that its Chinese subsidiary violated the Foreign Corrupt Practices Act by offering cash and other incentives to healthcare professionals to recommend Mead Johnson Nutrition products at government-owned hospitals. The company also failed to accurately record over \$2 million in improper payments made during a 5-year period.
Source: <http://www.sec.gov/news/pressrelease/2015-154.html>
22. ***July 28, The Boston Globe – (Massachusetts) Private information about research participants goes missing at McLean Hospital.*** McLean Hospital in Belmont, Massachusetts announced July 28 the information of 12,600 past and future brain donors as well as several family members may be compromised after 4 unencrypted data tapes containing private information at the Harvard Brain Tissue Resource Center went missing May 29. No patient information was breached, and the attorney general's office was notified July 28.
Source: <https://www.bostonglobe.com/business/2015/07/28/private-information-about-research-participants-goes-missing-mclean-hospital/1SHYJiOPJ0M3NIZbfVYfoJ/story.html>

For additional stories, see items [32](#) and [35](#)

Government Facilities Sector

23. ***July 28, University of Minnesota Center for Infectious Disease Research and Policy – (National) CDC: DoD anthrax errors involved 575 shipments.*** A total of 575 separate shipments of potentially live *Bacillus anthracis* (BA) samples were sent by a U.S. Army lab in Utah over the past decade, the Centers for Disease Control and Prevention official testified to a U.S. House subcommittee July 28. A Department of Defense official also reported a total of 31 U.S. lab workers were treated for possible exposure to the live samples, an increase from the 21 cases reported July 27.
Source: <http://www.cidrap.umn.edu/news-perspective/2015/07/cdc-dod-anthrax-errors-involved-575-shipments>
24. ***July 28, Arizona Republic – (Arizona) AZ Attorney General employees evacuated Statewide in bomb threats.*** Law enforcement officials are investigating a series of bomb threats targeting Arizona Attorney General Office employees, forcing statewide evacuations of all Attorney General Office locations July 28. Employees were able to return to their offices at varying times throughout the day as sites were cleared by

police and bomb-sniffing dogs.

Source:

<http://www.azcentral.com/story/news/local/phoenix/breaking/2015/07/28/bomb-threat-evacuates-attorney-generals-office/30786327/>

25. *July 28, U.S. Department of Justice* – (Florida) **Florida resident charged with attempting to use weapon of mass destruction.** A self-professed Islamic State adherent was charged with attempting to use a weapon of mass destruction against a person or property within the U.S. July 28 after planning to remotely detonate a timer bomb on a public beach in Key West. The suspect was arrested July 27 after taking possession of an inert device.

Source: <http://www.justice.gov/opa/pr/florida-resident-charged-attempting-use-weapon-mass-destruction>

26. *July 27, SC Magazine* – (Georgia) **Breach affects 3,000 clients enrolled in Georgia State program.** The personal data of approximately 3,000 clients of the Community Care Services Program in Georgia was potentially compromised June 8 after the Division of Aging Services accidentally emailed the information to a contracted provider not authorized to view the information. The recipients of the email did not access the information, and all affected clients have been notified.

Source: <http://www.scmagazine.com/breach-affects-3000-clients-enrolled-in-georgia-state-program/article/428766/>

For additional stories, see items [6](#), [32](#), and [35](#)

Emergency Services Sector

27. *July 28, Associated Press* – (Iowa) **Weeks after escape, inmates at Iowa maximum-security prison still face ‘restricted movement’.** The Iowa State Penitentiary in Fort Madison remains under lockdown July 28 after a convicted armed robber escaped from a top security cell July 5. Officials stated the lockdown will remain in place “per security concerns and operational needs.”

Source:

<http://www.greenfieldreporter.com/view/story/fbc91fd23d7b492c85e6c9892901f4d4/I-A--Escaped-Iowa-Inmate>

28. *July 28, WPVI 6 Philadelphia* – (Pennsylvania; New Jersey) **Police: man who led cops on 2 hour chase stole underwear.** A New Jersey man was charged July 28 after leading three different State police agencies on a two-hour car chase July 27 after stealing underwear from a Shop Rite store in Brooklawn, New Jersey. No injuries were reported.

Source: <http://6abc.com/news/police-man-who-led-cops-on-2-hour-chase-stole-underwear/887199/>

Information Technology Sector

29. *July 29, Securityweek* – (International) **Russian hacker tool uses legitimate Web**

services to hide attacks: FireEye. Security researchers from FireEye discovered that the APT29 threat group is employing a malicious backdoor dubbed “HAMMERTOSS” that utilizes a multi-stage process involving social media, steganography, and PowerShell to hide malicious activity within legitimate network traffic. Researchers believe that the backdoor is only being deployed against critical targets, possibly as a backup in case other tools fail or are disrupted.
Source: <http://www.securityweek.com/russian-hacker-tool-uses-legitimate-web-services-hide-attacks-fireeye>

30. *July 29, Securityweek* – (International) **BIND update patches critical DoS vulnerability.** The Internet Systems Consortium released updates for the popular BIND Domain Name System (DNS) software addressing a critical remotely exploitable vulnerability in the handling of TKEY recorded queries in which an attacker could use a specially crafted DNS packet to trigger a denial-of-service (DoS) condition.
Source: <http://www.securityweek.com/bind-update-patches-critical-dos-vulnerability>

31. *July 29, Softpedia* – (International) **Row Hammer DRAM bug now exploitable via JavaScript, most DDR3 memory chips vulnerable.** Security researchers from universities in Austria and France released findings revealing that the Row Hammer exploit can be initiated and actively exploited remotely via JavaScript, making it the first documented “remote software-induced hardware-fault attack.”
Source: <http://news.softpedia.com/news/row-hammer-dram-bug-now-exploitable-via-javascript-488050.shtml>

32. *July 29, Securityweek* – (International) **Black Vine espionage group attacked aerospace, energy, healthcare industries.** Security researchers from Symantec reported that the Black Vine espionage group responsible for the 2014 Anthem system breach has been active since 2012, used custom-built malware, zero-day exploits, and watering hole attacks to target organizations across the aerospace, healthcare, energy, military, defense, finance, agriculture, and technology industries, primarily in the U.S.
Source: <http://www.securityweek.com/anthem-hackers-targeted-multiple-industries-2012-symantec>

33. *July 29, The Register* – (International) **Microsoft admits critical .NET Framework 4.6 bug, issues workaround.** Microsoft released a workaround addressing a critical codegen bug for those running 64-bit processes on .NET Framework 4.6, in which incorrect parameters could be passed, leading to unpredictable results.
Source:
http://www.theregister.co.uk/2015/07/29/microsoft_acknowledges_net_framework_46_critical_bug_issues_workaround/

34. *July 29, Homeland Security News Wire* – (International) **Cellphones can steal data from isolated “air-gapped” computers.** Researchers at the Ben-Gurion University of the Negev Cyber Security Research Center discovered a way to use central processing unit (CPU) firmware-modification software to turn an air-gapped system into a cellular transmitting antenna, making it possible for any mobile phone infected with malicious

code to use GSM phone frequencies to steal data from infected air-gapped systems. Researchers recommended mitigation measures including defined “zones” where mobile phones and other devices are not allowed near at-risk air-gapped computers. Source: <http://www.homelandsecuritynewswire.com/dr20150729-cellphones-can-steal-data-from-isolated-airgapped-computers>

35. *July 29, Bloomberg* – (International) **China-tied hackers that hit U.S. said to breach United Airlines.** Investigators involved in a probe of a previously unreported May or June breach of United Airlines’ computer systems reported links between the hackers and the Chinese threat group that perpetrated the theft of security-clearance records from the U.S. Office of Personnel Management and medical data from Anthem Inc., as well as at least seven other travel and health insurance organizations. Officials believe that the breach may have compromised movement data of millions of Americans and opened the airline’s systems to future disruptions and attacks.
Source: <http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines>

36. *July 28, IDG News Service* – (International) **Xen patches new virtual-machine escape vulnerability.** The Xen Project released updates for its virtualization software addressing a vulnerability in the CD-ROM drive emulation feature of the QEMU open-source hardware emulator that could allow an attacker to bypass the security barrier between virtual machines and their host operating systems (OS).
Source: http://www.computerworld.com/article/2952638/security/xen-patches-new-virtual-machine-escape-vulnerability.html#tk.rss_security

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

37. *July 28, Jersey Journal* – (New Jersey) **800 Verizon customers in Bayonne without service after fiber optic cable is damaged, company says.** A Verizon Wireless spokesman reported that an estimated 800 customers in Bayonne are without phone, Internet, and TV service after a fiber optic cable was accidentally damaged July 28. Crews are working to repair the damaged cable and hope to have service restored later in the day.
Source:
http://www.nj.com/hudson/index.ssf/2015/07/verizon_customers_without_service_after_fiber_cabl.html

For additional stories, see items [34](#) and [41](#)

Commercial Facilities Sector

38. *July 29, Jersey Journal* – (New Jersey) **Overnight fire displaces 4 families, damages East Newark municipal garage.** A 3-alarm fire in East Newark, New Jersey displaced 4 families from a town duplex and damaged a municipal garage July 28, after the fire began on the left side of the building. The cause of the fire is under investigation.
Source:
http://www.nj.com/hudson/index.ssf/2015/07/overnight_fire_displaces_3_families_damage_munici.html

39. *July 29, KTRK 13 Houston* – (Texas) **Families displaced following massive four-alarm fire in NW Houston.** The Gentry House Apartments in Houston sustained extensive damage after a 4-alarm fire destroyed the building and displaced up to 80 families. Over 120 firefighters responded to the incident, leaving 3 injured with non-life threatening wounds.
Source: <http://abc13.com/news/four-alarm-fire-rips-through-nw-houston-apartment-complex/889528/>

40. *July 29, KCRA 3 Sacramento* – (California) **Lake Berryessa flare-up prompts additional evacuations, stirs fears.** A three-week old wildfire in Solano County prompted the evacuation of 200 residents of surrounding homes after the fire burned 150 acres outside the containment lines near residential areas, July 28. Fire crews are working to extinguish the flames with 80 percent containment.
Source: <http://www.kcra.com/news/wildfire-near-lake-berryessa-flares-up-again/34403920>

41. *July 28, Associated Press* – (California) **Bomb threat forces evacuation of CHP building in LA.** Approximately 60 people from the California Highway Patrol communications center in Los Angeles were evacuated for over 2 hours July 28 due to a bomb threat. Bomb-sniffing dogs and several police crews responded to the incident and found no explosive device.
Source: <http://www.sfgate.com/news/article/Bomb-threat-forces-evacuation-of-CHP-building-in-6411318.php>

42. *July 28, KTXL 40 Sacramento* – (California) **Crews get a handle on fire burning at South Sacramento Recycling Center.** A 3-alarm fire at the Sierra Waste Recycling and Transfer Center in South Sacramento prompted fire crews to remain onsite for several hours extinguishing hot spots July 28. No injuries were reported.
Source: <http://fox40.com/2015/07/28/fire-burning-at-recycling-center-in-south-sacramento/>

Dams Sector

Nothing to report



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions: Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List: Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List: Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.